REMARKS

Applicants hereby reply to the Office Action dated October 4, 2005 within the shortened three-month period for reply. Claims 18-25 and 35-37 were pending in the application and the Examiner rejects claims 18-25 and 35-37. Support for the amendments to the claims and specification may be found in the originally-filed specification, claims, and figures. No new matter has been introduced by these amendments. Reconsideration of this application is respectfully requested.

Rejections Under 35 U.S.C. § 112, ¶ 1

Claims 35-37 stand rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement. Specifically, the Examiner asserts that Applicants' argument stating that the specification supports a signed challenge string and a digital certificate "contradicts the clear teaching of paragraph 54, where Applicants equate the two, or at least requires one be an instance of the other (A signed challenge string (e.g., digital certificate)" (page 4, paragraph 1). Applicants respectfully traverse this rejection.

The distinctions between a digital certificate and a challenge string are well known in the art. A digital certificate is a universally structured message that contains information about the identity of the certificate owner, who it was issued by, a unique serial number, valid dates, and an encrypted "fingerprint" that can be used to verify the contents of the certificate. Digital certificates are issued by trusted third parties, known as a Certificate Authority (CA). Digital certificates have a fixed structure as to be universally accepted and processed across diverse computing platforms and software applications. As such, it would not be possible to modify the structure of the certificate (e.g., adding a signed challenge string), without adversely impacting how the certificate is processed. (*See,* http://www.sec-1.com/glossary/d.html, printed on December 20, 2005, attached hereto as Exhibit A.)

A challenge string, as is known to those skilled in the art, is a request for information (or response). Specifically, in the context of the present invention, a challenge string is a request for information regarding the identity of a user or computing system. Typically, a challenge string is sent by a host computer and will often prompt a user to enter specific credentials such as, for example, a user ID and password combination. The credentials are then used to encrypt the

challenge string using a private key (signature). The signed challenge string is then sent to the issuing host computer, decrypted and verified. A challenge string is typically encrypted and decrypted using a combination of public and private keys to ensure that integrity is maintained. (*See*, http://www.sec-1.com/glossary/c.html, printed on December 20, 2005, attached hereto as Exhibit B.)

As previously argued, Applicants maintain that the specification clearly enables the digital certificate and the signed challenge string as two distinct messages. For example, paragraph 14 states that the "challenge string is signed and transmitted with the digital certificate." (emphasis added) Further, paragraph 38 states that "the communication device 10 is configured with software to enable the smart card reader 12 to read the smart card 14 data and to communicate a signed challenge string and digital certificate to the host system 300". (emphasis added) Moreover, paragraph 39 states that "[T]he host system sends the user a challenge string (e.g., code with time-stamped feature) to the user 1. When the user 1 enters his or her PIN number the digital certificate is accessed, the challenge string is signed and returned, along with the digital certificate, to the host system 300." (emphasis added)

The Examiner further states that the "specification is also silent regarding some sort of comparison." However, in Applicants Reply dated February 3, 2005, paragraph 57 was amended to clarify that a user may be authenticated "by comparing the digital certificate to the signed challenge string or by comparing either the digital certificate or the signed challenge string to a third data set stored in the user and/or account information database tables." Thus, in light of the arguments presented as well as the amendment and support found in the specification, claim 35 is enabled to those skilled in the relevant art and Applicants request withdrawal of the rejection of claim 35.

Applicants assert that dependent claims 36 and 37, which depend from independent claim 35, are allowable for at least the same reasons as set forth above regarding independent claim 35, as well as in view of their own respective features.

Rejections Under 35 U.S.C. § 112, ¶ 2

Claims 35-37 also stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the

Applicants regard as the invention. Specifically, the Examiner asserts that Applicants previously filed arguments stating that the challenge string and digital certificate are distinct data contradicts the teachings of paragraph 54, where, "Applicant equates the two, or at least requires one be an instance of the other" (page 4, item 7). Applicants respectfully traverse this rejection.

Applicants maintain that claims 35-37 comply with 35 U.S.C. § 112, second paragraph for the same reasons as stated above. A digital certificate and signed challenge string are clearly known in the art as being distinct messages, and as previously stated, the combination of the two would likely render the digital certificate inoperable.

The Examiner further asserts that the specification, "is also silent regarding some sort of comparison, therefore in order to be considered distinct, the claim should include language such as, 'not one in the same' or 'different' (page 5, paragraph 1).

In the Applicants Reply dated February 3, 2005, paragraph 57 was amended to clarify that a user may be authenticated "by comparing the digital certificate to the signed challenge string or by comparing either the digital certificate or the signed challenge string to a third data set stored in the user and/or account information database tables." However to further clarify that the digital certificate and challenge string are not one in the same, Applicants have amended claim 35 according to the Examiner's suggestion.

Applicants assert that dependent claims 36 and 37, which depend from independent claim 35, are allowable for at least the same reasons as set forth above regarding independent claim 35, as well as in view of their own respective features.

Rejections Under 35 U.S.C. § 103

Claims 18-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Payne et al., U.S. Patent No. 5,715,314 ("Payne") in view of Purpura, U.S. Patent No. 6,421,768 ("Purpura"). Applicants traverse this rejection.

Payne discloses a system for facilitating purchases and payment transactions over a network. The Payne system includes a buyer computer, a merchant computer and a payment computer interconnected over a network. Payne further discloses a buyer selecting a product to purchase, wherein the selected product has a corresponding payment URL. The payment URL further comprises a domain identifier, payment amount, merchant computer identifier, merchant

account, various timestamps, buyer network address and a payment URL authenticator. Payne discloses that the payment URL authenticator is a hash being a defined key shared between the merchant and the operator of the payment computer. In other words, the hash itself is irrelevant to the purchase transaction details in that it only serves to authenticate the payment URL in order to ensure that the source of the payment URL is a legitimate merchant.

Payne discloses a hash (URL authenticator) being encompassed within a grouping of data (payment URL). Payne does not disclose a grouping of data (payment URL) being encompassed within a hash (URL authenticator) (column 5, lines 42-46). This is an important distinction because according to the teaching of Payne, the source of the data may be ensured by verifying that the URL authenticator was created by the content of the payment URL (column 5, lines 57-60); however, the integrity of the data encompassed within the payment URL itself is not ensured. Thus, the Payne reference is limited to providing assurance of the source of data (URL authenticator) and does not teach the use of a hash to facilitate the secure submission of a payment request, or the use of a hash to identify a transaction account to be charged in a transaction. As such, neither Payne, Purpura, nor any combination thereof, disclose or suggest at least, "communicating said secondary transaction number over said authenticated communication channel to said merchant, wherein said merchant submits a payment request based on said secondary transaction account number," as recited by independent claim 18.

Applicants assert that dependent claims 19 and 20 depend from independent claim 18 and are differentiated from the cited references for at least the same reasons as set forth above, as well as in view of their own respective features.

Claims 21-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Payne in view of Purpura, and in further view of Gifford, U.S. Patent No. 5,724,424 ("Gifford"). Applicants traverse this rejection.

Applicants assert, as explained above, that neither Payne, Purpura, Gifford, nor any combination thereof, disclose or suggest at least "communicating said secondary transaction number over said authenticated communication channel to said merchant, wherein said merchant submits a payment request based on said secondary transaction account number," as similarly recited by independent claim 18 and 23. Moreover, Claims 21 and 22 depend from independent claim 18 and claims 24 and 25 depend from independent claim 23, so claims 21-22 and 24-25 are

differentiated from the cited references for at least the reasons described above, as well as in view of their own respective features.

Claims 35-37 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Payne in view of Gifford. Applicants traverse this rejection.

Applicants assert that neither Payne, Gifford, nor any combination thereof, disclose or suggest at least "retrieving from said merchant a signed challenge string and a digital certificate originating from a user, wherein said challenge string and said digital certificate are not one in the same and, wherein said user is authenticated by comparing said signed challenge string and said digital certificate," as recited by independent claim 35. Moreover, claims 36 and 37 depend from independent claim 35, thus are differentiated from the cited references for at least the reasons described above, as well as in view of their own respective features.

In view of the above remarks and amendments, Applicants respectfully submit that all pending claims properly set forth that which Applicants regard as their invention and are allowable over the cited references. Accordingly, Applicants respectfully request allowance of the pending claims. The Examiner is invited to telephone the undersigned at the Examiner's convenience, if that would help further prosecution of the subject Application. Applicants authorize and respectfully request that any fees due be charged to Deposit Account No. 19-2814.

Respectfully submitted,

Dated: December 20, 2005

By:  57,413
Howard Sobelman
Reg. No. 39,038

SNELL & WILMER L.L.P.
400 E. Van Buren
One Arizona Center
Phoenix, Arizona 85004
Phone: 602-382-6228
Fax: 602-382-6070
Email: hsobelman@swlaw.com